9110-9N

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2020-0015]

Privacy Act of 1974; System of Records

AGENCY: Privacy Office, U.S. Department of Homeland Security.

ACTION: Notice of a New System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the U.S. Department of Homeland Security (DHS) proposes to establish a new DHS system of records titled, "U.S. Department of Homeland Security/ALL-046 Counterintelligence Program System of Records." This system of records allows DHS to collect and maintain records as part of the unified Counterintelligence Program across the Department. "Counterintelligence" is defined as information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of Foreign Intelligence Entities. DHS will use the system to facilitate counterintelligence functions including analysis, production, collections, investigative activities, operations, and functional support.

DATES: Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This new system will be effective upon publication. New routine uses will be effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number DHS-2020-0015 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.

- Mail: Constantina Kozanas, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

Instructions: All submissions received must include the agency name and docket number DHS-2020-0015. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Robert Hale, (202) 447-3984, CI.Question@hq.dhs.gov, Assistant Director, Enterprise Program Management, Counterintelligence Mission Center, Office of Intelligence and Analysis, 3801 Nebraska Avenue, Washington, D.C. 20528-0655. For privacy questions, please contact: Constantina Kozanas, (202) 343-1717, Privacy@hq.dhs.gov, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. sec. 552a, U.S. Department of Homeland Security (DHS) proposes to issue a new DHS system of records titled, "DHS/ALL-046 Counterintelligence Program System of Records."

DHS developed the Counterintelligence (CI) Program to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of Foreign Intelligence Entities (FIE). FIEs are known or suspected foreign state or non-state organizations or persons that conduct intelligence activities to acquire information about the United States, block or impair intelligence collection by the United States Government, influence United States policy, or disrupt systems and programs owned or operated by or within the United States, all of

which may impact or influence DHS operations and missions. The term includes foreign intelligence and security services, international terrorists, transnational criminal organizations, and drug trafficking organizations conducting intelligence-related activities.

DHS is creating this new CI program system of records to account for the expansion of the Department's CI program beyond the Office of Intelligence and Analysis (I&A) and the United States Coast Guard (USCG) to include Cybersecurity and Infrastructure Security Agency (CISA), Countering Weapons of Mass Destruction Office (CWMD), Federal Emergency Management Agency (FEMA), Federal Protective Service (FPS), Transportation Security Administration (TSA), U.S. Customs and Border Protection (CBP), U.S. Citizenship and Immigration Services (USCIS), U.S. Immigration and Customs Enforcement (ICE), and U.S. Secret Service (USSS).

Some DHS counterintelligence records previously covered under the DHS/IA-001 Enterprise Records System (ERS) system of records notice (SORN) will now be part of the Department's CI Program SORN. This notice does not rescind, revoke, or supersede the ERS SORN insofar as program offices in I&A will continue to maintain records separate from the CI program within that system of records.

The DHS CI Program derives its authorities from those provided to the Secretary of Homeland Security and to the Under Secretary for Intelligence and Analysis (USIA). The additional counterintelligence authorities provided to the USCG are not further shared with the rest of the DHS CI Program and are not restricted based on the limitations applied to I&A. Other DHS Components and offices in the DHS CI Program also retain their individual authorities and capabilities provided to those Components through statute, executive order, or DHS Delegation (*e.g*. TSA retains its authorities regarding transportation security and these authorities are not impacted by TSA's inclusion in the DHS CI Program).

The DHS CI Program derives its authorities primarily from Executive Order 12333, United States Intelligence Activities, which authorizes all members of the Intelligence Community to collect information concerning, and conduct activities to protect against, amongst other things, intelligence activities directed against the United States. All members of the Intelligence Community are further tasked with protecting the security of intelligence related activities, information, installations, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Intelligence Community elements as are necessary. Pursuant to Executive Order 12333, DHS's I&A is specifically authorized to collect (overtly or through publicly available sources) analyze, produce, and disseminate foreign intelligence and counterintelligence, including defense and defense-related information and intelligence to support national and departmental missions. In addition, Executive Order 12333 authorizes the Commandant of the Coast Guard to conduct counterintelligence activities, including through clandestine means. USCG intelligence authorities are functionally derived from Executive Order 13286, Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security.

The key distinction between the authorities for I&A and the USCG, specifically as it relates to collection of counterintelligence information, rests in the authority for USCG to collect counterintelligence using clandestine means, while I&A is only permitted to collect from overt or publicly available sources. The USCG is the only DHS component with the authority to conduct clandestine counterintelligence activities.

In addition to Executive Order 12333, the Homeland Security Act of 2002, codified at 6 U.S.C. 121-126, authorizes the USIA's role as the DHS Counterintelligence Executive. Furthermore, 6 U.S.C. 124d authorizes the DHS Intelligence Components (defined in 6 U.S.C. 101(11) as any element or entity (i.e., DHS Component) that

collects, gathers, processes, analyzes, produces, or disseminates intelligence information within the scope of the Information Sharing Environment or National Intelligence) to support and implement the intelligence mission of the Department, as led by the USIA. The DHS CI Program is part of the overall DHS intelligence mission.

Counterintelligence collections within the DHS CI Program (I&A, USCG, and all other Component CI programs) are undertaken as part of an integrated national and departmental effort. The DHS CI Program follows the Intelligence Community model for conducting counterintelligence, as described in Intelligence Community Directive 750 – Counterintelligence Program and other National Counterintelligence Security Center guidance. The DHS CI Program performs a variety of functions to fulfill its mission, including investigations, information collections, operations, analysis and production, and supporting functional services.

The DHS CI Program collects personally identifiable information (PII) directly from DHS employees and contractors via in-person interviews, from individuals outside of DHS who may have information relevant to a CI matter, government-controlled and public data aggregators, forensic examination of documents and electronic media, and anonymous tips and leads provided via email, telephone, and written notes or letters. As relates to CI investigations and operations, PII may be used to identify individuals who are involved in, witness to, or knowledgeable of CI-related activities that are the subject of a CI investigation or operation by the DHS CI Program or other federal law enforcement or intelligence agencies where there is a DHS equity. CI analytical products generally contain very limited amounts of PII, with sources and individuals referenced in a finished intelligence product anonymized to the greatest extent possible. Furthermore, the DHS CI Program provides DHS employees with CI awareness training, during which PII is collected directly from DHS employees in order to maintain a record of when CI awareness training was last received.

Consistent with DHS's information sharing mission, information stored in the DHS/ALL-046 Counterintelligence Program System of Records may be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

Additionally, DHS is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act elsewhere in the Federal Register. This newly established system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, The JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/ALL-046 Counterintelligence Program System of Records. In accordance with 5 U.S.C. sec. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER: U.S. Department of Homeland Security (DHS) DHS/ALL-046 Counterintelligence Program System of Records.

SECURITY CLASSIFICATION: Unclassified and Classified.

SYSTEM LOCATION: Records are maintained at several DHS Headquarters and Component locations in Washington, D.C. and field offices.

SYSTEM MANAGER(S): Robert Hale, Assistant Director, Enterprise Program Management, (202) 447-3984, CI.Question@hq.dhs.gov, Counterintelligence Mission Center, Office of Intelligence and Analysis, U.S. Department of Homeland Security, Washington, D.C. 20528.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title II and Title VIII, section 892 of the Homeland Security Act of 2002, Public Law 107-296, 116 Stat. 2135 (Nov. 25, 2002), as amended (6 U.S.C. 121, et seq.); Executive Order 12333, United States Intelligence Activities, 46 Fed. Reg. 59941 (December 4, 1981), *reprinted as amended* in 73 Fed. Reg. 45325 (July 30, 2008); Executive Order 13526, Classified National Security Information, 75 Fed. Reg. 707 (January 5, 2010); Executive Order 13556, Controlled Unclassified Information, 75 Fed. Reg. 68675 (November 9, 2010); and Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, 70 Fed. Reg. 62023 (October 27, 2005).

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to collect, store and maintain records related to, and in furtherance of, the counterintelligence collections and activities of the DHS CI Program. DHS will use this system to conduct administrative inquiries to identify, analyze, and neutralize foreign intelligence threats to DHS personnel, facilities, equipment, networks, information and activities; report on foreign

contacts and travel, including briefings and debriefings; conduct counterintelligence investigative activities and produce intelligence on foreign intelligence entities; provide counterintelligence awareness training; and other activities relating to the DHS CI Program's responsibilities.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

- Current and former DHS employees, contractors, consultants, detailees, interns, applicants for employment, and other individuals provided authorized access to DHS facilities, systems, or sensitive or classified information;
- Individuals who are known, reasonably believed to be, or are suspected of being, involved in or linked to:
    - intelligence activities, or other individuals known or suspected of engaging in intelligence activities, on behalf of FIEs;
    - officers or employees of, or otherwise acting for or on behalf of, a foreign government or element thereof, foreign organizations, or foreign persons;
    - officers, employees, or members of an organization reasonably believed to be owned or controlled directly or indirectly by a foreign power; or
    - clandestine intelligence activities, sabotage, assassinations, or international terrorist activities.
- Individuals reasonably believed to be targets, hostages, or victims of international terrorist organizations, transnational criminal organizations, or drug trafficking organizations;
- Individuals who are closely associated with the above categories (*e.g.*, immediate family members, members of a household, business partners); and
- Individuals who voluntarily request assistance or information, through any means, from the DHS CI Program, or individuals who voluntarily provide information

concerning any of the activities above, which may threaten or otherwise affect homeland security.

CATEGORIES OF RECORDS IN THE SYSTEM: The system may collect the following types of information if related to CI:

- Classified and unclassified intelligence (national intelligence, foreign intelligence, and counterintelligence), counterterrorism, homeland security, and related law enforcement information, including source records and the reporting and results of any analysis of this information, obtained from all agencies, components and organizations of the Federal government, including the IC; foreign governments, organizations or entities, and international organizations; State, local, tribal and territorial government agencies (including law enforcement agencies); and private sector entities;
- Information provided by record subjects and individual members of the public;
- Information obtained from the Terrorist Screening Center, the National Counterterrorism Center, or from other organizations about individuals known or reasonably suspected of being engaged in conduct constituting, preparing for, aiding, or relating to terrorism;
- Information obtained from the National Counterintelligence Security Center, the Federal Bureau of Investigation, or from other organizations about individuals known or reasonably suspected of being engaged in conduct associated with espionage, other intelligence activities, sabotage, or assassinations;
- Active and historical law enforcement investigative information;
- Information related to lawful DHS security investigations, including authorized physical, personnel, and communications security investigations, and information systems security analysis and reporting;
- Operational and administrative records, including correspondence records;

- Financial information, when relevant to an authorized intelligence, counterterrorism, homeland security, or related law enforcement activity;
- Public source data such as that contained in media, including periodicals, newspapers, broadcast transcripts, and other public reports and commercial databases;
- Publicly available social media handles and aliases, associated identifiable information, and search results; and
- Metadata, which may include but is not limited to transaction date, time, location, and frequency.

Examples of information related to the “Categories of Individuals" listed above may include:

- Individual’s name and alias(es);
- Date and place of birth;
- Gender;
- Country of citizenship;
- Country of nationality;
- Country of residence;
- A-Number(s);
- E-mail address;
- SSN;
- Vehicular information;
- Government issued identification information (*i.e.*, passport, driver’s license),
    - Document type;
    - Issuing organization;
    - Driver’s license;
    - Document number; and

    - Expiration date.
- Physical characteristics (height, weight, race, eye and hair color, ethnicity, identifying marks like tattoos or birthmarks);
- Biometric information (*e.g.,* fingerprints, photographs) and other information used to conduct background and security checks;
- Physical and mailing addresses (to include U.S. and foreign);
- Phone and fax numbers (including mobile phone numbers);
- Records regarding organization membership(s) or affiliation(s);
- Employment history;
- Results from intelligence analysis related to counterintelligence;
- Background investigative reports and supporting documentation, including criminal background, medical, and financial data;
- Family relationships (*e.g.,* parent, spouse, sibling, child, other dependents);
- Criminal history;
- Flight information;
- Border crossing information;
- Reports on foreign contacts;
- Records and information from government data systems or retrieved from commercial data providers in the course of intelligence research, analysis, and reporting;
- Immigration and visa information; and
- Investigative files containing allegations and complaints; witness statements; transcripts of electronic monitoring; subpoenas and legal opinions and advice; reports of investigation; reports of criminal, civil, and administrative actions taken as a result of the investigation; and other relevant evidence; handwriting exemplars, laboratory analyses of inks and papers; handwriting analyses;

information, reports or opinions from the forensic examination of documentary and digital media evidence; polygraph case files; search warrants and search warrant returns; indictments; certified inventories of property held as evidence; sworn and unsworn witness statements; state, local, and foreign criminal investigative information and reports; names and telephone numbers of individuals intercepted by electronic, mechanical, or other device under the provisions of 18 U.S.C. sec. 2510 et seq compiled during the lawful course of a criminal or civil investigation.

Records will also include those relating to:

- management and coordination of DHS counterintelligence systems and activities;
- analytical, operational, biographic, policy, management, training, administrative matters and operational support related to DHS counterintelligence, force protection, critical infrastructure protection, research and technology protection, threat analysis, counter-narcotics and risk assessments; and
- architecture and operation of DHS counterintelligence information systems.
- reports of investigation, collection, statements of individuals, affidavits, correspondence, and other documentation pertaining to investigative or analytical efforts by DHS and other U.S. government agencies to identify or counter foreign intelligence and international terrorist threats to DHS and to the United States.
- records maintained in ad hoc or temporary databases established to support certain investigations, task forces or analytical projects.

RECORD SOURCE CATEGORIES: Federal, state, local, territorial, tribal, or other domestic agencies, foreign agencies, multinational or non-governmental organizations, critical infrastructure owners and operators, private sector entities and organizations, individuals, commercial data providers, and public sources such as social media, news media outlets, and the Internet.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. sec. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. sec. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including the U.S. Attorneys Offices, or other federal agencies conducting litigation or proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity, only when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

B. To a congressional office with information from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. secs. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals,

DHS (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To another Federal agency or Federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

G. To an appropriate Federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

I. To representatives of the Department of Justice and other U.S. Government entities, to the extent necessary to obtain their advice on any matter that is within their

official responsibilities, authorities, and missions, in order to provide support to DHS's CI Program and the purposes of this system.

J. To any Federal, state, local, tribal, territorial, foreign, or multinational government or agency, or appropriate private sector individuals and organizations, with responsibilities relating to homeland security, including responsibilities to counter, deter, prevent, prepare for, respond to, or recover from a natural or manmade threat, including an act of terrorism, or to assist in or facilitate the coordination of homeland security threat awareness, assessment, analysis, deterrence, prevention, preemption, and response.

K. To a Federal, state, local, tribal, or territorial government or agency lawfully engaged in the collection of intelligence (including national intelligence, foreign intelligence, and counterintelligence), counterterrorism, homeland security, law enforcement or law enforcement intelligence, and other information, when disclosure is undertaken for intelligence, counterterrorism, homeland security, or related law enforcement purposes, as authorized by U.S. Law or Executive Order, and in accordance with applicable disclosure policies.

L. To any other agency within the Intelligence Community, as defined in Executive Order 12333, as amended, for the purpose of allowing that agency to determine whether the information is relevant and necessary to its mission-related responsibilities and in accordance with that agency's classified or unclassified implementing procedures promulgated pursuant to such orders and directives, or any other statute, Executive Order or directive of general applicability.

M. To a Federal, state, local, tribal, territorial, foreign, or multinational government or agency, or other entity, including, as appropriate, certain private sector individuals and organizations, when disclosure is in furtherance of the CI Program and DHS information sharing responsibilities under the Homeland Security Act of 2002, as amended, the Intelligence Reform and Terrorism Prevention Act of 2004, the National

Security Act of 1947, as amended, Executive Order 12333, as amended, or any successor order, national security directive, intelligence community directive, other directive applicable to DHS, and any classified or unclassified implementing procedures promulgated pursuant to such orders and directives, or any other statute, Executive Order or directive of general applicability, and where such disclosure is otherwise compatible with the purpose for which the record was originally acquired or created by DHS.

N. To an appropriate Federal, State, local, tribal, territorial, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit and when disclosure is appropriate to the proper performance of the official duties of the person making the request.

O. To the President's Foreign Intelligence Advisory Board, the Intelligence Oversight Board, any successor organizations, and any intelligence oversight entities established by the President, when disclosure will assist these entities in the performance of their oversight functions.

P. To foreign persons or foreign government agencies, international organizations, and multinational agencies or entities, under circumstances or for purposes mandated or imposed by Federal statute, treaty, or other international agreement or arrangement.

Q. To any individual, organization, or entity, as appropriate, to notify them of a serious threat to homeland security for the purpose of guarding them against or responding to such a threat, or when there is a reason to believe that the recipient is or

could become the target of a particular threat, to the extent the information is relevant to the protection of life, health, or property.

R. To any Federal government agency when documents or other information obtained from that agency are used in compiling the particular record, the record is also relevant to the official responsibilities of that agency, and there otherwise exists a need for that agency to know the information in the performance of its official functions.

S. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by an individual's name or other identifier, including unique identifying numbers assigned by DHS or other government agencies.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are retained and disposed of in accordance with approved records retentions schedules. Records on U.S. Persons, as defined in Executive Order 12333, are retained so long as there is a mission need, in accordance with N1-563-09-7-1. If DHS determines that U.S. Person record meets the two-part test, as described in N1-563-09-7-1, the records must be reviewed annually to determine whether there is still a mission need to retain the information. The majority of the DHS CI Program has 180 days from

the date U.S. Person information is first collected to determine whether it meets the two-part test.

The exception is USCG, where, pursuant to COMDTINST M3820.12, "Coast Guard Intelligence Activities", USCG originators of intelligence products have 90 days from the date of collection of USPER data to determine whether the information may be permanently retained within the USCG authorized procedures. USCG is working to update this instruction, and under the new version, will be permitted up to 5 years to determine if the USPER data may be permanently retained. At the anniversary date (or any time beforehand) a record is first certified as U.S. Person information can be reviewed and certified that there is still a mission need to retain the information. The anniversary date will then be set for an additional year out. This can go on for as long as the information is deemed necessary for the mission. Once certification has been removed, such records are temporary and must be destroyed and deleted immediately upon removal of certification. Certified and categorized records reaching the expiration date without review/renewal one year from date of categorization are temporary and must be destroyed and deleted upon that one-year cutoff. Finally, uncategorized records that do not meet the required two-part test are temporary and must be destroyed and deleted within 180 days (90 days for USCG) from the date the information is collected.

Interception, Monitoring and Recording of Wire and Oral Communication Records are retained in accordance with N1-563-08-5, and are temporary. Records are cutoff at the end of the calendar year in which the record was created, and are destroyed 10 years after cutoff.

Clip Reports are non-records, and are destroyed or deleted when no longer needed for reference.

Finished Intelligence Case Files are retained in accordance with N1-563-07-16-4, and are permanent. Records cutoff date is at the end of the calendar year in which the

case is closed and are transferred to the National Archives for permanent retention 20 years after such cutoff date.

Raw Reporting Files are retained in accordance with N1-563-07-16-3, and are temporary. Records cutoff date is at end of calendar year such records are collected and are destroyed or deleted 30 years after such cutoff date.

Counterintelligence Case Files are retained in accordance with N1-563-08-4-1, and are temporary. Records cutoff date is the end of the fiscal year of when the case has been closed and are destroyed 20 years after such cutoff date.

Non-Referral Files are retained in accordance with N1-563-08-4-3, and are temporary. Records are destroyed when 5 years old from first collected.

Certification File records are retained in accordance with N1-563-08-11-1, and are temporary. Records cutoff date is the end of the calendar year in which certification was received. Records are to be destroyed when 10 years old or 10 years after completion of a specific training program or upon separation or transfer of employee, whichever is sooner.

Mission-Related Training records are retained in accordance with N1-563-08-11-2, and are temporary. Records cutoff date is at the end of the calendar year in which course or material is superseded and are destroyed or deleted 30 years after cutoff date.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES: As described below, this system of records is exempt from the notification, access, and amendment provisions of the Privacy Act, and the Judicial Redress Act if applicable. However, DHS will consider individual requests to determine whether or not information may be released. Individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the FOIA Officer for the Office of Intelligence and Analysis, whose contact information can be found at http://www.dhs.gov/foia under "Contacts Information." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, U.S. Department of Homeland Security, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provides a right of access, certain records about you may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under Title 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, an individual may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, the individual should:

- Explain why he or she believes the Department would have information being requested;

- Identify which component(s) of the Department he or she believes may have the information;
- Specify when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If the request is seeking records pertaining to another living individual, the request must include an authorization from the individual whose record is being requested, authorizing the release to the requester.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES: For records covered by the Privacy Act or covered JRA records, individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to the Department component that maintains the record, unless the record is not subject to amendment or correction. The request should identify each particular record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. If the individual believes that the same record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record.

NOTIFICATION PROCEDURES: See "Record Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (e)(12); (f); and (g)(1). Additionally, the

Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). When this system receives a record from another system exempted in that source system under Title 5 U.S.C. 552a(j)(2), 5 U.S.C. § 552a(k)(1), (k)(2), and (k)(5), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

HISTORY: None.

*****

Constantina Kozanas,

Chief Privacy Officer,

U.S. Department of Homeland Security.

[FR Doc. 2020-27315 Filed: 12/11/2020 8:45 am; Publication Date: 12/14/2020]